

On the Andrews congruence for the Fibonacci quotient

John Blythe Dobson (j.dobson@uwinnipeg.ca)

July 1, 2014

Abstract

We show that a congruence discovered by George E. Andrews in 1969 for the Fibonacci quotient directly implies a simpler congruence found by Hugh C. Williams in 1991.

Keywords: Fibonacci quotient, harmonic numbers

1 Introduction

In his celebrated 1969 study of the Fibonacci sequence ([1], p. 114), George E. Andrews gave two congruences modulo a prime p for divided Fibonacci numbers:

$$F_{p-1}/p \equiv 2 \left(\frac{-1}{p} \right) \sum_{\substack{j=-p+1 \\ j \equiv 5, 7 \pmod{10}}}^{p-1} \frac{\left(\frac{j+1}{5} \right) \left(\frac{-1}{j} \right)}{p-j} \quad [p \equiv \pm 1 \pmod{5}; p > 5] \quad (1a)$$

$$F_{p+1}/p \equiv 2 \left(\frac{-1}{p} \right) \sum_{\substack{j=-p+1 \\ j \equiv 1, 5 \pmod{10}}}^{p-1} \frac{\left(\frac{j+1}{5} \right) \left(\frac{-1}{j} \right)}{p-j} \quad [p \equiv \pm 2 \pmod{5}; p > 5]. \quad (1b)$$

Andrews takes the Jacobi symbol $\left(\frac{-1}{p} \right)$ in the sense $(-1)^{(p-1)/2}$, while some authors take it as $(-1)^{(|p|-1)/2}$. Together these congruences characterize the Fibonacci quotient $F_{p-(\frac{5}{p})}/p$ for $p \neq 5$, since $\left(\frac{5}{p} \right) = 1$ and -1 in the two cases, respectively. Andrews noted the resemblance of the sums in these results with the sums of reciprocals that occur in the congruence for the Fermat quotient in the classic study of Eisenstein [5]. Later Hugh C. Williams, using (as he himself notes) a quite different method, was able in his 1982 paper on the Fibonacci quotient [10] to derive a simpler congruence exactly analogous to Eisenstein's, and in his 1991 paper treating quotients of Lucas numbers ([11], p. 440, eq. 4.7) he further simplified this to

$$F_{p-(\frac{5}{p})}/p \equiv \frac{2}{5} \sum_{j=\lfloor p/5 \rfloor + 1}^{\lfloor 2p/5 \rfloor} \frac{1}{j} \pmod{p} \quad [p > 5]. \quad (2)$$

Williams's result can also be viewed as a statement about a special type of harmonic number H , since it can be written

$$F_{p-(\frac{5}{p})}/p \equiv \frac{2}{5} \left\{ H_{\lfloor 2p/5 \rfloor} - H_{\lfloor p/5 \rfloor} \right\} \pmod{p} \quad [p > 5]. \quad (3)$$

We regard Williams's elegant formulation as canonical, as it is the simplest possible when the terms in the sum are constrained to be of like sign and equal weight. This property facilitates comparison with other results pertaining to the Fermat quotient, particularly those discussed in [6] and [2] in relation to the first case of Fermat's Last Theorem.

As it does not appear to have been generally recognized that Andrews's result implies (2), and as the exercise of deriving (2) directly from (1a & b) may perhaps suggest possibilities for the simplification of similar results in the literature, we shall demonstrate how this can be done. We do so with unavoidable foreknowledge of (2), but without introducing any additional facts about the Fibonacci numbers. The only apparatus required follows from a 1905 paper of Lerch [7].

2 Some preliminaries

We shall make use of a notation originally introduced by Lerch, but with the shift in index adopted in [2] and most recent writings:

$$s(k, N) = \sum_{\substack{j=\lfloor \frac{kp}{N} \rfloor + 1 \\ j \neq p}}^{\lfloor \frac{(k+1)p}{N} \rfloor} \frac{1}{j}, \quad (4)$$

where it is always assumed that p is sufficiently large that $s(k, N)$ contains at least one element; the provision $j \neq p$ is necessary when $k+1 = N$, though we shall not encounter that situation here. In this notation, therefore, the sum in the right-hand side of (2) can be written as $s(1, 5)$. We shall frequently make use of the trivial fact that $s(k, N) \equiv -s(N-1-k, N) \pmod{p}$.

Lerch ([7], p. 476, equations 14 and 15), correcting work of Sylvester, pretty much explicitly writes out the relation $2 \cdot s(0, 5) + s(1, 5) \equiv -\frac{5}{2} \cdot q_p(5)$, where $q_p(5)$ is the Fermat quotient of p to the base 5. While we shall not pursue this matter here, it is thus evident that the evaluation of $s(1, 5)$ simultaneously settled the evaluation of $s(0, 5)$. This result, and the core formulae of Lerch's paper, supply a number of relationships between sums of the type defined in (4), and these are greatly extended in a recent paper of Dilcher and Skula [3].

We shall need a lemma in this vein:

Lemma 1.

$$-s(1, 10) + 2 \cdot s(2, 10) + 3 \cdot s(3, 10) \equiv 0 \pmod{p}. \quad (5)$$

Proof. The ingredients needed for this lemma are developed using only ideas from Lerch [7] in [3], pp. 20–21, Proposition 3.1. Earlier, it had been proved in a less elementary way, and employing a slightly different notation, in a paper of Skula ([8], p. 9, Theorem 3.2), which gives:

$$2 \cdot s(0, 10) + 3 \cdot s(1, 10) + 2 \cdot s(2, 10) + 3 \cdot s(3, 10) + 2 \cdot s(4, 10) \equiv 0 \pmod{p}.$$

$$s(0, 10) + 2 \cdot s(1, 10) + s(4, 10) \equiv 0 \pmod{p}.$$

Subtracting twice the second row from the first gives (5). \square

We shall also need a formula for a sum which, under various notations, has made frequent appearances in the literature of the Fermat quotient. If $K(r, N)$ represents the sum of the terms in $s(0, 1)$, i.e. the sum of the terms in the set $\left\{1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{p-1}\right\}$, whose denominators are congruent to $rp \pmod{N}$ for a prime p and $r < N$, then

Lemma 2.

$$K(r, N) \equiv \frac{1}{N} \cdot s(N - r, N) \pmod{p}. \quad (6)$$

Proof. This formula was given in 1995 by Zhi-Hong Sun ([9], pt. 3, p. 90, Corollary 3.1), though it may be older. For an elementary proof using ideas from Lerch [7] see [4], §4. \square

This relation, which defines an association between terms characterized by a congruential condition on denominators lying in the interval $\{1, p-1\}$, and a consecutive block of terms $s(k, N)$, permits simplification of many published results involving sums of reciprocals. One is usually interested in sums of terms whose denominators belong to some fixed residue class t , so if p is invertible modulo N and this inverse is p' , one sets $r = tp'$.

3 The main result

We are now ready to derive (2) from (1a & b). First, we rewrite (1a & b) in a more explicit form, still modulo p but with the summations now confined to the range $\{1, p-1\}$:

$$\begin{aligned}
& F_{p-1}/p \\
& \equiv 2 \left(\frac{-1}{p} \right) \left\{ \sum_{\substack{j \equiv 15 \\ \text{mod } 20}} \frac{2}{j} - \sum_{\substack{j \equiv 5 \\ \text{mod } 20}} \frac{2}{j} + \sum_{\substack{j \equiv 13, 17 \\ \text{mod } 20}} \frac{1}{j} - \sum_{\substack{j \equiv 3, 7 \\ \text{mod } 20}} \frac{1}{j} \right\} \quad (7a) \\
& [p \equiv \pm 1 \text{ mod } 5; p > 5]
\end{aligned}$$

$$\begin{aligned}
& F_{p+1}/p \\
& \equiv 2 \left(\frac{-1}{p} \right) \left\{ \sum_{\substack{j \equiv 15 \\ \text{mod } 20}} \frac{2}{j} - \sum_{\substack{j \equiv 5 \\ \text{mod } 20}} \frac{2}{j} + \sum_{\substack{j \equiv 1, 9 \\ \text{mod } 20}} \frac{1}{j} - \sum_{\substack{j \equiv 11, 19 \\ \text{mod } 20}} \frac{1}{j} \right\} \\
& [p \equiv \pm 2 \pmod{5}; p > 5] \quad (7b)
\end{aligned}$$

The first row covers the cases $p \equiv 1, 9, 11, 19 \pmod{20}$, and the second row the cases $p \equiv 3, 7, 13, 17 \pmod{20}$; the eight cases must be split out in order to determine the values of the Jacobi symbol $\left(\frac{-1}{p}\right)$. Next, we apply Lemma 2 to each of the component sums, letting t be the residue class modulo 20 specified for each summation, and for $p \equiv 1, 9, 11, 19, 3, 7, 13, 17 \pmod{20}$, taking $p' = 1, 9, 11, 19, 7, 3, 17, 13$, respectively (the first four residues are their own inverses, being the square roots of unity). Routine calculations then establish that for all eight cases of p , (7a & b) reduce (after rearrangement) to

$$\begin{aligned}
& F_{p-(\frac{5}{p})}/p \\
& \equiv \frac{1}{10} \{s(2, 20) + s(3, 20) + 2 \cdot s(4, 20) + 2 \cdot s(5, 20) + s(6, 20) + s(7, 20)\} \quad (8) \\
& \pmod{p} \quad [p > 5].
\end{aligned}$$

In view of the definition of $s(k, N)$, it is clear that when k and N are both even, we have $s(k, N) + s(k+1, N) = s(\frac{k}{2}, \frac{N}{2})$. Thus (8) condenses to

$$F_{p-(\frac{5}{p})}/p \equiv \frac{1}{10} \{s(1, 10) + 2 \cdot s(2, 10) + s(3, 10)\} \pmod{p} \quad [p > 5],$$

and finally, adding one tenth of (5) to this gives

$$F_{p-(\frac{5}{p})}/p \equiv \frac{1}{10} \{4 \cdot s(2, 10) + 4 \cdot s(3, 10)\} \equiv \frac{2}{5} \cdot s(1, 5) \pmod{p} \quad [p > 5],$$

which is equivalent to (2), as required.

References

- [1] George E. Andrews [misprinted as George H. Andrews], “Some formulae for the Fibonacci sequence with generalizations,” *Fibonacci Quart.* **7** (1969), 113–130, 274 (correction).
- [2] Karl Dilcher & Ladislav Skula, “A new criterion for the first case of Fermat’s Last Theorem,” *Math. Comp.* **64** (1995), 363–392.
- [3] K. Dilcher & L. Skula, “Linear relations between certain sums of reciprocals modulo p ,” *Ann. Sci. Math. Québec* **35** (2011), 17–29.
- [4] John Blythe Dobson, “On Lerch’s formula for the Fermat quotient,” preprint at <http://arxiv.org/abs/1103.3907>.
- [5] [G.] Eisenstein, “Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definirt werden,” *Berichte Königl. Preuß. Akad. Wiss. Berlin* **15** (1850), 36–42.
- [6] Emma Lehmer. “On Congruences involving Bernoulli numbers and the quotients of Fermat and Wilson,” *Ann. of Math.* **39** (1938), 350–360.
- [7] M. Lerch, “Zur Theorie des Fermatschen Quotienten. . .,” *Math. Ann.* **60** (1905), 471–490.
- [8] Ladislav Skula, “A note on some relations among special sums of reciprocals modulo p ,” *Math. Slovaca* **58** (2008), 5–10.
- [9] Zhi-Hong Sun, “Combinatorial sum $\sum_{k \equiv r \pmod{m}} \binom{n}{k}$ and its applications in Number Theory” (in Chinese), *J. Nanjing Univ. Math. Biquarterly* **9** (1992), 227–240, **10** (1993), 205–118, **12** (1995), 90–102. A very full summary in English is available on the author’s website, at <http://www.hytc.cn/xsj1/szh/>.
- [10] H. C. Williams, “A note on the Fibonacci quotient. . .,” *Canad. Math. Bull.* **25** (1982), 366–370.
- [11] H. C. Williams, “Some formulas concerning the fundamental unit of a real quadratic field,” *Discrete Math.* **92** (1991), 431–440.